*BY ORDER OF THE COMMANDER*

*70TH INTELLIGENCE WING OPERATING INSTRUCTION 31-403*

*9 AUGUST 2002*

***Security***

***COLUMBIA ANNEX (CANX) SECURITY PROCEDURES***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally.

---

OPR: 70 IW/SF (MSgt Sheila M. Dixon) Certified by: 70 IW/SF (SMSgt Robert L. Norman)
Pages: 10
Distribution: L (FOUO)

---

This Wing Operating Instruction implements AFPD 31-4, *Information Security*. It also implements DoD Directive 5200.1, Information Security Program Regulation; and complements the guidance set forth in DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*; and AFI 31-40, *Information Security Program Management.* This operating instruction applies to all military members, DoD civilians, and contractors assigned to, on temporary duty to, or visiting 70 IW staff offices located at the Columbia Annex (CANX). This instruction outlines the Physical Security procedures needed to protect personnel and property working in or visiting the CANX. It identifies procedures for the protection, storage, transmission and destruction of classified material as prescribed by the aforementioned instructions and directives.

**1. GENERAL:** It is the responsibility of every assigned, attached or visiting member to properly safeguard sensitive information entrusted to him/her and to immediately report instances of suspected compromise or known risk that pose a threat to the integrity of the Information Security Program within the CANX. This Operating Instruction (OI) identifies procedures for access to the CANX Sensitive Compartmented Information Facility (SCIF), outlines opening and closing procedures, visitor control and implements classified material controls. In the event of a suspected compromise or risk to classified material, the person(s) discovering the incident must take control of the material(s) and safeguard them until the material(s) can be properly stored. Notification of the incident must be reported to the Wing Staff Security Manager immediately. During non-duty hours, the Security Manager will be notified through the Wing Readiness Center, 301-688-5151. Adherence to the CANX day-to-day security procedures is imperative and supports the wing's overall Information Security Program. Formal access control and existing protective measures for the protection of classified or otherwise sensitive information are set forth in local guidance.

**2. THE SPECIAL SECURITY REPRESENTATIVE (SSR) WILL:**

2.1. Manage access control and the end-of-day security process for the staff assigned to the CANX.

2.2. Provide advice and assistance to Division Chiefs, and unit personnel working within the CANX.

2.3. Assist in "no-notice" inspections (conducted by Wing Staff Security Manager) on all areas that handle, process, or store classified material.

2.4. Monitor personnel security actions and ensure that all personnel working within the SCIF properly display their entry credential.

2.5. Ensure that escort officials take all necessary precautions for the protection of sensitive information.

2.6. Be responsible for the timely update of the NSA Key and Alarm Tracking System (KATS) program.

2.7. Each month, collect and file completed Standard Form 701, **Activity Security Checklist**.

2.8. Ensure that the requirements identified in 70 IW Instruction 31-402 are met.

**3. SCIF Opening.**

3.1. Entry into the SCIF requires only one authorized person. The person needing to open the SCIF must be on the SCIF access authorization list (Security Manager manages the access authorization list). The main point of entry and exit for the SCIF is door number CX1DO42 and the key to be requested is CX36A. Once the SCIF has been accessed, the “open/closed” sign will be flipped to reflect that the SCIF is occupied.

3.2. **SCIF Closing.**

3.2.1. Each Division Chief must ensure that his/her work center is secured at the end of each duty day. Each person is responsible for his or her particular workspace and material. All classified material must be put away (i.e. locked in a cabinet, bookcase, desk drawer or GSA approved safe) and the STU-III keys removed from all units and properly stored in the assigned key box.

3.2.2. A SF 701 for each Division assigned to the CANX (DO, LG, SC and XP etc.) will be placed at the main entrance. The last person leaving that particular division must complete the SF 701 and initial where necessary. Additionally, the individual completing their divisional SF 701 must review all SF’s 701 attached to the clipboard. The purpose of the review will be to see if the divisional representative is the last person inside the SCIF. The collocation of the divisional SFs 701 at the main entrance does not preclude each duty section from maintaining its own SF 701 if it chooses to. However, the process of maintaining duplicate SF’s 701 then becomes redundant and the duty section SF 701 cannot be considered representative of or a replacement for the divisional SF 701.

3.2.3. If after review of the divisional SF’s 701 at the main entrance and inspection of the work spaces, it is discovered that the divisional representative is the last person within the SCIF, he/she will be responsible for conducting an end-of-day check of the entire facility to ensure that it is secured for the evening. Specific procedures are as follows:

3.2.3.1. At the end of each duty day, each exterior door will be secured and the exterior mounted “open/closed” magnet, at each door, changed to “closed.” Personnel tasked with securing the SCIF will ensure that each division is secure *i.e.* the SF 701 (Activity Security Checklist) completed and initialed. CX1DO42 will be locked, the magnetic sign changed to “closed,” the SF 701 is completed and the key returned to the guard at the facility’s main point of entry. NOTE: An entry is not required on the SF 701 on non-duty days such as weekends

and holidays (provided the facility is not used that day).

3.2.4. Following these procedures will ensure that the facility is secured at the end of each duty day and prevent the inadvertent locking of the SCIF while personnel are still working within their duty section.

3.2.5. The success of the SCIF closure process is heavily dependent upon the level of importance and support it receives from the division chiefs assigned to and working within the secure spaces of the CANX. The SSR and 70 IW Chief, Security Forces will randomly conduct unannounced facility security checks to validate the success of the closure process and document instances of noncompliance with established procedures. Division chiefs will be notified immediately of discrepancies noted within their area. A report of the discrepancy will be generated and the appropriate level of command notified, when necessary.

## 4. CIRCULATION CONTROL.

### 4.1. UNESCORTED ENTRY:

4.1.1. Unescorted entry is limited to properly badged personnel assigned to the 70th Intelligence Wing, TDY personnel and visitors that have their clearance verification on file with NSA Q142. Unescorted access to the SCIF does not translate to “need to know,” therefore personnel are reminded to be judicious with the information they possess and to always be conscious of their immediate surroundings.

4.1.2. At all times, personnel working within the SCIF are responsible for safeguarding sensitive information with the required level of protection and accountability. Day-to-day working procedures within each duty section will be organized and conducted in a manner that denies uncleared visitors both hands-on access and audio access to sensitive information. When removed from storage, and not in use, classified material will be protected by the use of the appropriate cover sheet; this also applies to privacy act information.

### 4.2. ESCORTED ENTRY:

4.2.1. All occupants of the SCIF will be briefed that one or more uncleared visitors will be entering the SCIF and the areas to be visited. Sufficient time will be allowed so that a sanitization of the area can be affected for both the area to be visited and the area that must be used as a thoroughfare. Visitors will be logged in on the visitor log (located at main entrance), the flashing/rotating red light will be activated and the visitor(s) escorted at all times. Each time that the uncleared visitor(s) transits through a particular duty section, the escort official will make a verbal warning “Red Badge in the area” to the duty-section occupants.

4.2.2. The escort official must maintain positive control of the escortee at all times (maintain visual contact). Upon completion of the visit, the visitor will be escorted out, the red light turned off and the visitor log annotated.

## 5. INFORMATION PROTECTION.

5.1. Each division will use the Standard Form (SF) 701, Activity Security Checklist, for end-of-day security checks. The SF 701 will include STU-III telephones and all other equipment/areas used to store and/or process classified information. As an added safety measure, all heat producing electrical items will be "checked" and turned off, where appropriate. The adoption of a “clean-desk (no docu-

ments on desk)" policy by section chiefs is encouraged, but it is the responsibility of each individual to ensure that no classified information is left on his/her workstation at the end of the duty day (CANX office space is not cleared for open storage). All classified material must be secured (in a locked container) at the end of the duty day. The last person leaving the division will attest to the sanitization of the duty section by annotating the SF 701 at the main entrance. The Standard Form 702, **Security Container Check Sheet**, will be annotated each time a security container/key box is opened and/or closed. The SF 702 will be annotated each duty day whether or not the security container/key box is opened. In those instances when the security container/key box is not opened on a particular duty day, the phrase "not opened" will be annotated on the SF 702 and the "checked by" section annotated as required.

5.2. Classified material will not be removed from designated work areas for work at home without proper authorization, packaging, and courier certification.

5.3. Telephone security should always be considered. Each person tasked to use the STU-III and NSTS phones must understand usage procedures prior to using them. When using administrative phones, ensure the phrase "Phone's Up" and "Phone's Down" is used to notify coworkers of telephone usage. Maximum use of the NSTS telephone is encouraged and should not be used solely for the purpose of discussing sensitive information.

5.4. Magnetic media will be processed through their duty section Workgroup Manager upon initial entry or permanent removal from the SCIF. The Communications and Information System Division (SC) will promulgate guidance for magnetic media control.

5.5. Prior to removing documents from the SCIF, the transporter of the information is responsible for ensuring that no classified information is mistakenly attached to the documents. In those instances where it is the intent of the transporter to remove classified documents from the SCIF, all precautions will be taken and the document properly wrapped prior to exiting the SCIF. In all instances however, the 70 IW Form 1, Accountability Log, (**Attachment 2**) will be used and serve as a source document attesting to the classification of the documents removed from the SCIF.

## 6. FACSIMILE EQUIPMENT.

6.1. Facsimile Equipment Transmission. The sender is responsible for reviewing each document for classified content before transmitting over a facsimile machine. If the document contains classified material, the sender must ensure that the document is appropriately marked. The sender must also ensure that the facsimile machine used to transmit and receive the transmission is approved at the appropriate classification level. The STU-III must also have a Crypto Ignition Key (CIK) equal to or greater to the information to be processed.

6.2. When transmitting a classified fax, the following procedures will be used:

6.2.1. Fill out the logbook.

6.2.2. Verify the classification of the fax and pass on that information to the intended recipient.

6.2.3. Turn on the fax machine.

6.2.4. Pick up the STU III and dial the fax number.

6.2.5. Tell the receiving end the number of pages.

6.2.6. Press the secure button on the STU III.

6.2.7. Once in secure mode, verify the recipient's level of classification by checking the STU III liquid crystal display (LCD).

6.2.8. Engage the Voice/Data button if in the voice mode.

6.2.9. Place the fax face down in the feeder (ensure that a cover sheet is used), then press the start button.

6.2.10. Once the fax is complete, verbally verify that the fax, in its entirety, was received. If all is well, hang up and turn off the fax machine.

6.2.11. If transmission problems occur, contact the SSR and Unit Security Manager immediately.

6.3. When receiving a classified fax, the following procedures will be used:

6.3.1. Answer the STU III, ask the classification and number of pages to be transmitted, and then ensure that the fax machine is on.

6.3.2. Verify the classification via the cover sheet.

6.3.3. Once the fax is complete, verbally verify that the fax was received, in its entirety.

6.3.4. Turn off the fax machine, hang up the STU III and fill out the logbook.

## 7. HANDCARRY OF CLASSIFIED MATERIAL.

7.1. CANX division chiefs will notify the Wing Security Manager when they have designated someone as an authorized courier. The Security Manager will arrange for the designee to be trained, ensure that a DD Form 2501, **Courier Authorization Card**, is issued and add the member's name to the list of designated couriers.

7.2. The handcarrying of classified material will not be used as a convenience; it will be kept to an absolute minimum and will be used only as a last resort. One person may serve as a courier; however, the division chief must consider the operational need and associated risks involved when authorizing a single individual to handcarry classified material. Circumstances such as volume of material, mode of travel, environment and material sensitivity should be considered in making that determination. If there is any question regarding a courier's ability to retain positive control of the material, two people should be employed.

7.3. Those tasked with courier duties will ensure that they attend the scheduled training before handcarrying any classified material into or out of the CANX. Couriers will:

7.3.1. Proceed quickly and directly to their approved and specific destination.

7.3.2. Avoid visits to non-secure areas and not conduct unofficial business while enroute.

7.3.3. Retain physical control of classified material at all times until the material is delivered and/or secured at its final destination.

7.3.4. Ensure that classified material is protected from loss, exposure to unauthorized people, or other forms of compromise.

7.3.5. Ensure that the classified material being handcarried is properly marked, wrapped, and labeled. The outer container will bear no address, classification or caveat markings. The package will be placed in a lockable container and the container tagged with the instructions "Property of the U.S. Government, DO NOT OPEN; if found call: (443) 479-3362 (collect)."

7.3.6. Provide an inventory of all handcarried classified material to a point of contact (within the area departed from) and notify that POC upon arrival at the intended destination.

## 8. REPRODUCTION OF CLASSIFIED MATERIAL.

8.1. All assigned personnel are authorized to reproduce Sensitive Compartmented Information (SCI) and up to Secret collateral material (unless told otherwise by their supervisor). Each time the copier is used to reproduce classified material, at least two blank sheets will be produced to ensure that no residual images are evident. Those blank sheets of paper will be considered "classified waste" and placed in a burn bag for disposal.

8.2. The copier will be located in an open and easily monitored area. Reproduction should be kept to a minimum and instances of excessive classified reproduction, reported to the security manager.

## 9. DESTRUCTION OF CLASSIFIED.

9.1. Burn bags will be used to hold all classified waste. If classified will be placed in the burn bag, the bag will be marked with the highest security classification of the information that will be placed in it. If SCI will be placed in the bag, the phrase "**CONTAINS SCI MATERIAL**," and the member's office symbol and telephone number will be clearly marked on the bag.

9.2. When a burn bag is filled, it will be sealed with staples or tape to prevent accidental tearing or breaking.

9.3. Secure burn bags at the end of each duty day and always afford them the protection commensurate with the level of information they contain (the burn bag takes on the highest classification of the information within). Burn bags can be disposed of each Monday and Wednesday between 0850 – 0910. The NSA truck used to transport classified waste, parks in the rear of the facility and is the only authorized recipient of our classified waste.

9.4. Annual Cleanout Day. ***Each division will observe the first Wednesday in December as the annual cleanout day.*** Each unit member and duty section should, as a matter of daily practice, destroy or transfer classified information no longer needed for mission support.

## 10. PROHIBITED ITEMS.

10.1. Prohibited items are those that constitute a physical or technical threat to NSA/CSS information, personnel and facilities. Unless approved by the Chief, Office of Security Services, or his/her designee, the following items are prohibited in NSA/CSS facilities:

10.1.1. Firearms and/or ammunition.

10.1.2. Explosives, incendiary substances, radioactive materials, flammable liquids, solids, gases, or other hazardous materials.

10.1.3. Personally-owned pagers and other like devices that can transmit.

10.1.4. Personally-owned cellular phones and telecommunication for the Deaf (TTD) devices.

10.1.5. Personally-owned test, measurement, and diagnostic equipment.

10.1.6. Personally-owned two way transmitting devices (e.g., CB, Ham radio, devices with infrared ports, etc.).

10.1.7. Personally-owned photographic and recording equipment (audio, video, optical) and associated information storage media.

10.1.8. Personally-owned computers (laptops, notebooks, etc.), and associated information storage media.

10.1.9. Personally-owned Personal Data Assistants (PDAs, Palm-Pilots, and other similar devices).

10.1.10. Personally-owned Information Storage Media includes, but is not limited to, disc storage media; magnetic tapes (audio, video, computer); 35mm slides; microfilm and microfiche; used carbon computer tape and typewriter ribbon; processed and unprocessed film; optical disks; and non-volatile, removable/transportable solid state media devices, such as flash memory cards.

10.1.11. Personally-owned music CDs, distinguished by the shiny silver color and manufacturer's artist label, are permitted. Read/write CDs are prohibited (gold in color).

## 11. Forms.

11.1. Prescribed Form. 70IW Form 1, **Accountability Log**.

JAMES O. POSS, Colonel, USAF
Commander

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

DoD 5200.1-R*, Information Security Program*

AFI 31-401, *Information Security Program Management*

NSA/CSS Reg 121-18, *Physical Security Requirements For Controlled Areas*

***Abbreviations and Acronyms***

**CANX—**Columbia Annex

**CIK—**Crypto Ignition Key

**GSA—**General Services Administration

**KATS—**Key and Alarm Tracking System

**LCD—**Liquid Crystal Display

**MAJCOM—**Major Command

**SCIF—**Sensitive Compartmented Facility

**SF—**Standard Form

**SSR—**Special Security Representative

**STU—**Secure Telephone Unit

## Attachment 2

## ACCOUNTABILITY LOG

**READ!** THIS FORM WILL BE USED IN EVERY INSTANCE WHERE DOCUMENTS ARE REMOVED FROM A SECURE ENVIRONMENT. THE INDIVIDUAL TAKING THIS PACKAGE OUTSIDE OF A SECURE AREA WILL PRINT, SIGN, DATE AND CHECK THE APPROPRIATE BOXES. IF THE PACKAGE CONTAINS CLASSIFIED MATERIAL, CHECK THE "Y" BOX, IF NOT, CHECK THE "N" BOX. **REMOVE SCI CLASSIFIED MATERIAL** AND CHECK THE APPROPRIATE BOX **BEFORE LEAVING** THE SECURE AREA (UNLESS THE PACKAGE WILL BE TRANSPORTED DIRECTLY TO ANOTHER SECURE AREA). **EACH** INDIVIDUAL HANDLING THIS PACKAGE **WILL** REVIEW THE CONTENTS AND **WILL** PRINT THEIR NAME, SIGN, DATE AND CHECK THE APPROPRIATE BOX.

IF THE PACKAGE CONTAINS COLLATERAL CLASSIFIED INFORMATION, I.E., NON- COMINT MATERIAL, THE HOLDER WILL ENSURE THE APPROPRIATE COVER SHEET IS ATTACHED AND THE INTENDED RECEPIENT IS AWARE OF THE PACKAGE'S CLASSIFICATION. COLLATERAL MATERIAL MAY BE TAKEN TO A NON SCIF AREA, PROVIDED THE HOLDER OF THE PACKAGE ENSURES THAT THE INTENDED RECIPIENT HAS THE NECESSARY SECURITY CLEARANCE AND IS MADE AWARE OF THE CONTENTS OF THE PACKAGE.

**NOTE:** THIS FORM WILL REMAIN WITH THE DOCUMENT/PACKAGE UNTIL IT HAS REACHED ITS FINAL DESTINATION. (DESTROY WHEN NO LONGER NEEDED)

THIS FORM MAY BE USED TO HOLD INDIVIDUALS ACCOUNTABLE FOR INADVERTENTLY OR INTENTIONALLY RELEASING OR TAKING CLASSIFIED MATERIAL OUTSIDE THE CONFINES OF AN APPROPRIATE SECURE AREA.

| NAME: (Last, First, MI) | SIGNATURE | SUBJECT (Unclassified) | DATE | Y | N |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**70 IW FORM 1, 20020809** *(EF-V1)*

**FOR OFFICIAL USE ONLY**